Filtrage P2P

Coppens, François

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2008

Document Version
le PDF de l'éditeur

Civ. Bruxelles, 29 juin 2007

Note d'observations de François Coppens[1]

DROIT D'AUTEUR – CESSATION – SOCIÉTÉ DE L'INFORMATION – INTERNET – *PEER-TO-PEER* – RESPONSABILITÉ – INTERMÉDIAIRE TECHNIQUE – VIE PRIVÉE – DONNÉES À CARACTÈRE PERSONNEL – CONFIDENTIALITÉ DES COMMUNICATIONS

Il existe des mesures techniques permettant aux intermédiaires ISP, dont les services sont utilisés pour l'échange non autorisé de fichiers électroniques musicaux grâce à des logiciels peer-to-peer, d'empêcher les atteintes à des droits d'auteur ainsi commises.

Ces mesures ne sont pas contraires à la loi du 8 décembre 1992 sur la protection des données à caractère personnel, ni au régime de responsabilité prévu par la directive 2000/31 (« dite commerce électronique »).

Des questions et des spéculations sur des évolutions techniques futures éventuelles ne peuvent aujourd'hui faire obstacle à une mesure de cessation dès lors que celle-ci s'avérerait actuellement techniquement possible et en mesure de produire un résultat.

L'action en cessation ne suppose aucun constat préalable d'une faute dans le chef de l'intermédiaire.

Il convient d'accorder un délai à l'intermédiaire pour se conformer à l'ordre de cessation. Le coût des mesures nécessaires au respect de l'ordre de cessation est à charge de l'intermédiaire.

• • •

Unauthorized exchanges of electronic musical files with peer-to-peer software are infringements on copyright. The intermediary ISP's are able, with technical measures, to prevent those infringements taking place on their networks.

These measures are not prohibited by the Law of 8 December 1992 (protection of personal data), nor are they contrary to the liability system established by directive 2000/31 ('electronic commerce directive').

Questions and speculations about eventual future technical evolutions shall not prevent a cessation measure that is at present technically possible and effective.

The cessation action does not require ascertaining a fault of the intermediary service provider.

The ISP must be given a period to implement the preventing order. The costs are to be supported by the ISP.

[1] Étudiant D.T.I.C.

Siège : M^me^ Heilporn

s.c.r.l. Société belge des auteurs (M^e^ Michaux) **c. s.a. Scarlet** (M^e^ Van Praet)

LES ANTÉCÉDENTS

Par citation du 24 juin 2004, la Sabam a formé une action en cessation fondée sur l'article 87, § 1^er^, de la L.D.A. relative aux droits d'auteur et aux droits voisins, dirigée contre la s.a. Tiscali aux fins d'entendre constater l'existence d'atteintes au droit d'auteur sur les œuvres musicales appartenant au répertoire de la Sabam du fait de l'échange non autorisé de fichiers électroniques musicaux illicites réalisés grâce à des logiciels dits *peer-to-peer*, atteintes commises au travers de l'utilisation des services de la s.a. Tiscali, d'entendre condamner celle-ci à faire cesser ces atteintes, en rendant impossible ou en paralysant toute forme d'envoi ou de réception par ses clients de fichiers reprenant une œuvre musicale, sans l'autorisation des ayant droits, au moyen d'un logiciel *peer to peer*, sous peine d'une astreinte de 25 000 EUR par jour ou partie de journée où la s.a. Tiscali ne respecterait pas le jugement à intervenir à partir du huitième jour suivant sa signification et de voir ordonner des mesures d'affichage sur le site internet de la s.a. Tiscali et de publication dans des quotidiens du jugement à intervenir.

La s.a. Tiscali a formé une demande reconventionnelle tendant à voir condamner la Sabam au paiement des sommes de 25 000 EUR pour procédure téméraire et vexatoire et de 25 000 EUR pour ses frais de défense.

Le tribunal de céans, après avoir rejeté l'exception d'incompétence *ratione materiae* soulevée par la s.a. Tiscali, a, dans son jugement du 26 novembre 2004 :

- admis que la Sabam justifiait d'un intérêt à diriger une action en cessation contre la s.a. Tiscali en sa qualité d'intermédiaire ISP dont il était allégué que les services étaient utilisés par des tiers pour porter atteinte à un droit d'auteur,
- dit établie l'existence d'atteintes au droit d'auteur sur les œuvres musicales faisant partie du répertoire de la Sabam du fait de l'échange non autorisé de fichiers électroniques musicaux grâce à des logiciels *peer to peer* et ce, au travers de l'utilisation du réseau internet de la s.a. Tiscali,
- rappelé que la constatation d'une atteinte au droit d'auteur contraint en principe le tribunal à en prononcer la cessation et que l'ordre de cessation doit mettre fin de manière effective à la situation illicite,
- estimé qu'il n'était pas suffisamment éclairé sur la faisabilité des mesures techniques qui pourraient être envisagées pour qu'il puisse concrètement être mis fin aux atteintes au droit d'auteur commises par les internautes utilisant les services de la s.a. Tiscali,

en conséquence de quoi, une expertise a été ordonnée, l'expert ayant pour mission de :

- « prendre connaissance de l'intégralité des rapports établis par HP, Cap Gemini et L. Golvers et d'examiner les solutions proposées dans ces rapports ;
- dire si les solutions envisagées dans ces rapports sont techniquement réalisables et si elles peuvent techniquement être mises en place sur les installations de la s.a. Tiscali ;
- dire si ces solutions permettent de filtrer uniquement les échanges illicites de fichiers électroniques ou bien concernent l'ensemble des utilisations via les logiciels *peer to peer* ;
- dire si d'autres dispositifs (de filtrages ou autres) peuvent être envisagés pour contrôler l'usage des logiciels *peer to peer* et le cas échéant de déterminer si ces dispositifs affecteraient l'ensemble des échanges internet ou seulement les échanges considérés comme illicites ;
- déterminer le coût des dispositifs qui sont envisagés ou qui pourraient l'être et la durée de leur mise en place ;
- répondre à toutes questions utiles des parties, les concilier si faire se peut et à défaut d'y parvenir, déposer son rapport au greffe du tribunal dans les trois mois de la mise en mouvement de l'expertise à la requête de la partie lapins diligente ».

Il a par ailleurs été réservé à statuer sur la demande reconventionnelle de la s.a. Ticali.

L'expert a déposé son rapport au greffe du tribunal de première instance le 3 janvier 2007.

La s.a. Tiscali a changé de dénomination et est devenue la s.a. Scarlet Extended.

DISCUSSION

1. Demande principale

1.1. Attendu que Scarlet reproche à la Sabam d'avoir attendu jusqu'au mois de mars 2006 avant d'avoir mis en mouvement l'expertise ; qu'elle estime dès lors que « l'urgence de la demande en cessation ne peut plus être présumée » et évoque un éventuel comportement abusif de la Sabam, dans la poursuite de la présente procédure ;

Attendu que l'action en cessation ne requiert pas l'urgence ; que le demandeur ne peut dès lors se voir opposer qu'il aurait tardé à agir (C. Dalcq, « Vers et pour une théorie générale du comme en référé », C.U.P. 2006, *Les actions comme en référé*, p. 60) ;

Que le 22 mai 2006, la Sabam a adressé à l'expert judiciaire une note technique d'introduction reprenant plusieurs solutions de blocage et de filtrage ;

Que l'on ne peut faire grief à la Sabam, qui est *a priori* moins informée en matière d'internet qu'un opérateur de télécommunication, d'avoir voulu apporter à l'expert un dossier complet ; que le nombre de solutions présentées à l'expert par la Sabam peut expliquer le temps mis par elle pour se constituer ce dossier ;

Que le retard dénoncé par Scarlet n'est lors pas constitutif d'un abus de droit ;

1.2. Attendu que dans son rapport, l'expert judiciaire a dégagé onze solutions « techniquement pertinentes à court terme pour le filtrage P2P », dont sept « applicables au réseau Scarlet » ;

Que parmi ces sept solutions, l'expert a estimé qu'une seule, « Audible Magic » (CopySense Network Appliance), « cherche à identifier le contenu musical protégé dans les flux P2P », les autres applications étant « des solutions de gestion de trafic, qui utilisent notamment et non exclusivement la reconnaissance d'application comme discriminant. Aucune de ces autres solutions de gestion n'a donc pour objectif de différencier le contenu véhiculé au sein de ces applications » ;

Que l'expert considère dès lors que « la solution proposée par la société Audible Magic est donc la seule à tenter de répondre à la problématique de manière spécifique » ;

Qu'il constate toutefois que :

- « la pérennité des solutions de filtrage d'application P2P est loin d'être assurée sur le moyen terme (2-3 ans) de par l'utilisation grandissante du cryptage dans ce type d'application »,
- la solution proposée par Audible Magic, « essentiellement destinée au monde éducatif n'est ... pas dimensionnée pour répondre au volume de trafic d'un F.A.I. (c'est-à-dire un fournisseur d'accès à internet) »,
- « le recours à cette technique dans le contexte F.A.I. induit de ce fait un coût d'acquisition et d'exploitation élevé pour compenser ce sous-dimensionnement », coût « qui est à mettre en regard avec la période pendant laquelle cette solution sera efficace, le cryptage... rendant cette solution également inefficace dans le cadre du filtrage en transit » ;

Attendu que sur la base de ces constatations, la Sabam considère qu'il existe dès lors plusieurs solutions permettant à Scarlet de mettre fin aux atteintes constatées ;

Que Scarlet estime pour sa part que les techniques auxquelles la Sabam se réfère ne sont pas aptes à empêcher l'échange non autorisé d'œuvres musicales dans la mesure où « la licéité d'une transmission est une donnée inaccessible à la technique » (il n'est pas possible de savoir si l'auteur de l'œuvre a consenti à la communication en cause ou si cette dernière peut être justifiée par une exception au droit d'auteur ou une licence légale) et où « l'identification même des œuvres échangées pourrait poser problème » en raison du cryptage des données transmises ;

Attendu qu'ainsi qu'il a déjà été rappelé dans le jugement du 26 novembre 2004, l'ordre de cessation doit produire un résultat en ce sens qu'il doit mettre fin de manière effective à la situation illicite (voy. implicitement Cass., 6 décembre 2001, *A&M*, 2002, p. 146 et la note de B. Michaux) ;

Qu'il faut qu'il existe des mesures techniquement possibles pour empêcher les atteintes au droit d'auteur ;

Que le rapport d'expertise, complété par les informations produites par la Sabam à son dossier, permet en l'espèce de conclure qu'il existe effectivement de telles mesures ;

Que l'expert a dégagé sept solutions applicables au réseau Scarlet dont six ont pour effet de bloquer l'utilisation *peer to peer* sans distinction du contenu (solutions de blocage) et dont une est une solution de filtrage qu'il considère comme étant la plus appropriée « à tenter de répondre à la problématique de manière spécifique » ;

Que relativement à cette dernière solution, la Sabam soutient, sans être contredite, que la solution Audible Magic, qui cherche selon l'expert « à identifier le contenu musical protégé dans les flux P2P » utilise une base de données « qui couvre plus de 70 % des chansons protégées échangées sur internet » ce qui correspond « en réalité à plus de 90 % du volume des fichiers musicaux illicites effectivement échangés sur internet » ;

Que la Sabam fournit par ailleurs la preuve que cette solution a d'ores et déjà été adoptée par « un des géants de l'internet », My Space, qui est « une des plates f ormes d'échanges les plus sollicitées par les internautes » pour bloquer l'utilisation non autorisée de contenus protégés par le droit d'auteur (voy. communiqué de presse et article de presse paru dans le *New York Times* du 13 février 2007) ; que Microsoft a par ailleurs également annoncé son intention d'utiliser « la technologie de tatouage numérique Copysense Network Appliance d'Audible Magic pour détecter et bloquer automatiquement tout contenu protégé » (voy. communiqué de presse et article paru sur Vnunet.com le 28 mars 2007) ; qu'enfin selon Audible Magic, « un ISP asiatique de premier plan a installé le dispositif Copysense Network Appliance d'Audible Magic sur son réseau pour évaluer la technologie et son potentiel dans le domaine de la large bande passante. Le test a été réalisé pendant l'été 2005. Le test a démontré que la technologie pouvait être utilisée pour identifier et filtrer le contenu protégé par le droit d'auteur sur son réseau » ;

Que ces éléments sont de nature à contredire la conclusion de l'expert (qui n'est appuyée d'aucun élément informatif) selon laquelle, la solution Audible Madic ne serait « pas dimensionnée pour répondre au volume de trafic d'un F.A.I. » ; que la Sabam produit en outre à son dossier une étude « Iometrix » démontrant la capacité d'Audible Magic de faire face à des volumes de trafic très importants avec un résultat de 99,3 à 100 % EUR de fichiers bloqués ;

Que la Sabam fait par ailleurs observer que si l'expert a émis des réserves quant à la pérennité des solutions en raison du cryptage des données, il a néanmoins admis, après avoir été interrogé sur ce point par la Sabam, qu'il n'avait pas examiné « l'aspect faisabilité (technique, temporelle, etc..) d'une encryption par les réseaux *peer to peer* » ; que la Sabam soutient que « la référence à l'encryption dans le cadre du *peer to peer* est abusive » puisque « l'accès massif au réseau *peer to peer* suppose nécessairement que le contenu du fichier recherché par l'internaute dans ce réseau soit lisible pour tous les participants. La lecture et le téléchargement de ces fichiers ne peut pas être limitée à un groupe restreint de personnes qui partagent un secret » ;

Que ces considérations techniques ne sont pas contestées par Scarlet Extended ;

Qu'en outre et plus fondamentalement, il échet de relever que la question d'un cryptage futur éventuel ne peut aujourd'hui faire obstacle à une mesure de cessation dès lors que celle-ci s'avérerait actuellement techniquement possible et en mesure de produire un résultat, comme c'est le cas en l'espèce ; que le secteur de l'internet est en constante évolution ; que le juge de la cessation ne peut tenir compte de spéculations sur des évolutions techniques futures éventuelles, d'autant que celles-ci pourraient également faire l'objet d'adaptations parallèles au niveau des mesures de blocages et de filtrage et notamment de la solution Audible Magic ;

Qu'enfin le coût moyen de la mise en œuvre de ces mesures ne semble pas excessif ; que selon l'expert, ce coût estimé sur une période de trois ans (durée de l'amortissement) et sur la base d'un nombre d'utilisateurs de l'ordre de 150 000 personnes ne devrait pas excéder 0,5 EUR par mois et par utilisateur ;

Qu'il résulte de l'ensemble de ces considérations qu'il existe effectivement à ce jour des mesures techniquement possibles pour empêcher les atteintes au droit d'auteur constatées dans le jugement du 26 novembre 2004 ;

Que certes, ces mesures pourraient sans doute également avoir comme conséquence marginale de bloquer certains échanges autorisés ; que la circonstance qu'une mesure de cessation affecte un ensemble d'informations dont certaines ne sont pas contrefaites (par

exemple un film, un livre, un CD...) n'empêche toutefois pas qu'il puisse être fait droit à celle-ci ; que, comme le tribunal de céans le relevait déjà dans son jugement du 26 novembre 2004, le juge de la cessation ne peut, sous réserve d'un abus de droit, refuser de prononcer la cessation de l'atteinte en recourant à une balance des intérêts qui pencherait en défaveur du plaignant (De Visscher et Michaux, *Précis du droit d'auteur et des droits voisins*, n° 635) ; que Scarlet ne démontre en l'espèce pas que la Sabam abuserait de ses droits en sollicitant lesdites mesures ; que la seule circonstance que le blocage affecterait certains contenus licites est insuffisant pour conclure à un abus de droit dans le chef de la Sabam ;

Attendu que la s.a. Scarlet Extended conteste néanmoins la possibilité pour le tribunal de céans d'ordonner la cessation en arguant de ce que :

– les mesures techniques sollicitées reviennent à lui imposer une obligation générale de surveillance de la totalité du trafic *peer to peer*, ce qui constituerait une charge permanente contraire à la législation sur le commerce électronique (directive 2000/31 et la loi du 11 mars 2003 qui la transpose),

– la mise en place de mesures de filtrage risque de lui faire perdre l'exonération de responsabilité pour l'activité de simple transport dont bénéficient les intermédiaires techniques en vertu de l'article 12 de la directive 2000/31,

– les mesures techniques sollicitées en ce qu'elles reviennent à « installer de façon permanente et systématique des appareils d'écoute » violeront les droits fondamentaux et plus particulièrement le droit à la vie privée, le droit, au secret de la correspondance et le droit à la liberté d'expression ;

Attendu que la directive 2000/31 du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur énonce en son article 15 que « les Etats membres ne doivent pas imposer aux prestataires... une obligation générale de surveiller les informations qu'ils transmettent ou stockent » (cette disposition a été transposée en droit interne par l'article 21, § 1er, de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information) ;

Que l'article 15, qui fait partie de la section 4 de la directive consacrée à la « Responsabilité des prestataires intermédiaires », vise à éviter que le juge national déduise une faute dans le chef du prestataire du fait de la simple présence sur ses réseaux d'une information illicite au motif qu'il aurait manqué à une obligation générale de surveiller toutes les informations quelconques qu'il transmet (C. De Preter, « Wie heeft nog boodschap aan de boodschap ? – De aansprakelijkheid van tussenpersonen onder de Wet Elektronische Handel », *A&M*, 2003, p. 256, spéc. p. 265) ;

Que cette disposition qui règle ainsi la question de la responsabilité du prestataire s'adresse toutefois exclusivement au juge de la responsabilité et est sans incidence sur le présent litige dans la mesure où l'action en cessation ne suppose aucun constat préalable d'une faute dans le chef de l'intermédiaire ;

Que la directive 2000/31 n'affecte en effet pas le pouvoir du juge de l'injonction et ne limite pas les mesures qui peuvent être prises par celui-ci à l'égard du prestataire ;

Que les dispositions de la directive 2000/31 sur la responsabilité des prestataires intermédiaires et partant l'interdiction d'imposer une obligation générale de surveillance « ne doivent en effet pas faire obstacle au développement et à la mise en œuvre effective, par les différentes parties concernées, de système technique de protection et d'identification ainsi que *d'instruments techniques de surveillance* rendus possibles par les techniques numériques » (voy. considérant 40 de la directive) ;

Que l'ordre de cessation n'impose pas à Scarlet de « surveiller » son réseau ;

Que les solutions identifiées par l'expert sont des « instruments techniques » qui se limitent à bloquer ou à filtrer certaines informations qui sont transmises sur le réseau de Scarlet ; qu'elles ne sont pas constitutives d'une obligation générale de surveiller le réseau ;

Qu'en faisant droit à l'ordre de cessation sollicité le tribunal de céans n'ordonne dès lors aucune mesure contraire à l'article 15 de la directive 2000/31 (voy. en ce sens F. Petillion, note sous Civ. Bruxelles, cess., 26 novembre 2004, *Computerrecht*, 2005, p. 65, spéc. p. 71) ;

Attendu en outre que c'est à tort que Scarlet estime que cette injonction aurait pour effet de lui faire perdre

l'exonération de responsabilité prévue à l'article 12 de la directive 2000/31 (article 18 de la loi du 11 mars 2003) qui bénéficie au prestataire dont l'activité se limite au simple transport ou de fourniture d'accès à internet à la condition notamment qu'il ne sélectionne ni ne modifie les informations faisant l'objet de la transmission ;

Que selon le considérant 45 de la directive 2000/31, « les limitations de responsabilité des prestataires de services intermédiaires prévues dans la présente directive sont sans préjudice de la possibilité d'actions en cessation de différents types. Ces actions en cessation peuvent notamment revêtir la forme de décisions de tribunaux... exigeant qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible » ;

Que le seul fait que l'instrument technique de filtrage laisserait passer des œuvres contrefaites du répertoire de la Sabam n'implique en outre nullement que ces œuvres auraient été sélectionnées par Scarlet ; qu'en effet le fait de ne pas parvenir à bloquer un contenu n'implique pas que ce contenu ait été sélectionné par l'intermédiaire à défaut pour celui-ci de cibler l'information en vue de la fournir à sa clientèle ; que la mesure de blocage a un caractère purement technique et automatique, l'intermédiaire n'opérant aucun rôle actif dans le filtrage ;

Que par ailleurs et à supposer même que Scarlet perde dans cette hypothèse le bénéfice de l'exonération, il ne s'en suivrait pas nécessairement que sa responsabilité serait engagée ; qu'il faudrait en effet encore démontrer une faute dans son chef ; que ce contentieux relèverait toutefois du seul juge de la responsabilité ;

Attendu enfin que les logiciels de filtrage et de blocage ne traitent en tant que tels aucune donnée à caractère personnel ; qu'à l'instar des logiciels antivirus ou antispam, ils sont de simples instruments techniques qui comme tels ne réalisent pas d'activités impliquant l'identification d'internautes ;

Qu'en outre la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel autorise en son article 5, *b,* le traitement de données à caractère personnel qui est nécessaire à l'exécution du contrat ; que les conditions générales de Scarlet auxquelles le contrat signé entre Scarlet et ses abonnés renvoie prévoient que le réseau ne peut être autorisé qu'à des fins prévues par la loi et qu'il est notamment interdit d'effectuer une connexion qui viole les droits d'auteur ; que Scarlet se réserve le droit de prendre des sanctions au cas où l'abonné enfreindrait cet engagement ; que l'installation de logiciels de filtrage ou de blocage qui impliqueraient une identification des internautes en rapport avec les opérations de filtrage ou de blocage ne contreviendrait dès lors pas à la loi du 8 décembre 1992 ;

Que le tribunal de céans n'aperçoit pour le surplus pas en quoi les logiciels de blocage ou de filtrage violeraient le droit « au secret de la correspondance » ou la liberté d'expression, Scarlet ne s'en expliquant au demeurant pas ;

Attendu qu'il résulte de l'ensemble de ces considérations que les mesures techniquement possibles pour empêcher les atteintes au droit d'auteur constatées dans le jugement du 26 novembre 2004 ne contreviennent pas aux dispositions légales invoquées par Scarlet ;

Qu'il convient dès lors de faire droit à l'ordre de cessation ;

Qu'un délai de six mois pour permettre à Scarlet de se conformer à l'ordre de cessation paraît raisonnable ; que selon les informations obtenues par la Sabam, le temps d'installation de la solution Audible Magic (solution la plus complexe) est, à dater de la commande, de quatre à six mois ;

Qu'il appartiendra à Scaret de communiquer par écrit à la Sabam dans ce même délai de six mois, le descriptif des mesures adoptées ;

Que l'astreinte se justifie dans son principe pour assurer une efficacité à la présente décision en ce qu'elle concerne l'ordre de cessation ; que seul un incitant financier sérieux peut en effet garantir l'exécution volontaire d'une condamnation de faire ; que son montant sera toutefois réduit à 2 500 EUR par jour de retard à dater de l'échéance du délai de 6 mois ;

Attendu que la mesure de publication doit réellement contribuer à la cessation ; que tel n'est pas le cas en l'espèce ; qu'il n'est en effet pas établi que la publication de la présente décision aura un effet plus dissuasif sur Scarlet ;

Attendu enfin que Scarlet soutient qu'il ne lui appartient pas de prendre en charge le coût relatif aux mesures techniques qui devraient être mises en place pour se conformer à l'ordre de cessation à défaut de base juridique l'y obligeant et de responsabilité établie dans son chef ; qu'elle entend dès lors imposer à la Sabam de supporter le coût des mesures qu'elle devrait prendre ;

Qu'il n'appartient en principe pas au juge de l'injonction de régler cette question ; qu'il lui suffit de constater l'existence de mesures techniquement possibles pour empêcher les atteintes au droit d'auteur ; qu'une fois ce constat fait, il ne peut, sous réserve d'un abus de droit, refuser de prononcer la cessation de l'atteinte ; que la prise en charge du coût, des mesures prises par le débiteur de l'injonction pour se conformer à celle-ci est la conséquence de l'ordre de cessation (voy. par analogie l'article 1248 du Code civil qui met à charge du débiteur les frais du paiement, c'est-à-dire les frais qu'occasionne l'exécution de l'obligation) ;

Qu'il ne peut en toute hypothèse être raisonnablement soutenu en l'espèce (et Scarlet ne le soutient au demeurant pas) que la Sabam abuserait de ses droits en considérant que le coût des mesures techniques doit être supporté par le débiteur desdites mesures, d'autant que celui-ci est, selon la directive 2001/29, « le mieux à même de mettre fin aux atteintes » et peut répercuter ce coût (estimé par l'expert à un maximum de 0,5 EUR par mois et par utilisateur durant trois ans) sur les internautes (alors que la Sabam ne dispose pas de cette même possibilité à défaut de pouvoir identifier les internautes contrevenants) ;

2. Demande reconventionnelle

Attendu que la s.a. Scarlet sollicite la condamnation de la Sabam au paiement de dommages et intérêts pour procédure téméraire et vexatoire ;

Qu'elle estime que la demande de la Sabam est uniquement destinée à lui nuire dans la mesure où elle n'a engagé de procédure qu'à son égard alors que d'autres fournisseurs d'internet, qui occupent une part nettement plus importante du marché sont également concernés et qu'aucune action n'a été entreprise contre les fournisseurs de logiciels *peer to peer* ;

Attendu que la demande principale étant déclarée fondée, elle n'a de ce seul fait rien de téméraire et vexatoire puisqu'elle exclut que la Sabam ait agi avec légèreté ou imprudence ;

Qu'au surplus, le fait que d'autres opérateurs ISP, voire même les fournisseurs de logiciels *peer to peer* ou encore les hébergeurs de sites web de ces fournisseurs, pourraient également faire l'objet d'une action en cessation ne porte pas atteinte au droit de la Sabam de diriger, dans un premier temps, son recours uniquement contre un seul des ISP dès lors qu'il n'est nullement démontré qu'en faisant ce choix, la Sabam n'aurait pas agi comme aurait dû le faire un justiciable prudent et diligent ;

Que pour des raisons financières compréhensibles, la Sabam a pu estimer opportun, dans un premier temps, de limiter son action à un seul ISP ;

Par ces motifs,

Nous, …

[…]

Condamnons la s.a. Scarlet Extended à faire cesser les atteintes au droit d'auteur constatées dans le jugement du 26 novembre 2004 en rendant impossible toute forme, au moyen d'un logiciel *peer to peer*, d'envoi ou de réception par ses clients de fichiers électroniques reprenant une œuvre musicale du répertoire de la Sabam, sous peine d'une astreinte de 2 500 EUR par jour où Scarlet ne respecterait pas le jugement après l'expiration d'un délai de six mois suivant sa signification ;

Condamnons la s.a. Scarlet Extended à communiquer par écrit à la Sabam dans les six mois de la signification du présent jugement le descriptif des mesures qu'elle appliquera en vue de respecter le jugement ;

Déboutons la Sabam du surplus de ses demandes ;

Disons la demande reconventionelle recevable mais non fondée ;

En déboutons la s.a. Scarlet Extended.

Note. – Dans cette affaire, une première décision avait déjà été prononcée le 26 novembre 2004, *A&M*, 2005/1, p. 49.

Note d'observations

Filtrage P2P : possibilités techniques et obstacles juridiques

INTRODUCTION

« Une fois de plus, la justice belge s'est montrée en ce début du mois de juillet disciple particulièrement zélée de la lutte contre le piratage, cette grande cause internationale dont chacun sait l'extrême importance et surtout la préséance sur certains droits fondamentaux comme le droit à la vie privée ou la liberté d'expression. Il s'agit en somme d'une sorte de version mineure de la lutte contre le terrorisme, c'est-à-dire d'un artéfact idéologique hors du temps et de l'espace, dénué de toute consistance et largement situé hors du champ juridique auquel il lui préfère les champs moral (c'est le mal qu'on combat) et politique (ceux qui refusent de s'engager au côté des vaillants pourfendeurs du mal sont des complices du mal) »[1].

Telle était l'introduction, volontiers provocatrice, d'un article intitulé « L'absurde croisade de la Sabam contre le *peer-to-peer* » trouvé au hasard sur internet, dans lequel l'auteur d'un blog livrait son sentiment sur l'affaire qui est l'objet de cette note.

La lutte contre l'échange illicite de musique sur internet tend il est vrai à susciter les antagonismes et les positions tranchées. Tandis que ses chevaliers se prévalent de la protection des auteurs, se posant en derniers remparts avant la mort de la création artistique, ses pourfendeurs craignent l'avènement de l'ère Big Brother au nom de la protection d'un système archaïque aux mains des multinationales du disque. Tant de pages – et de pixels – ont été noircis dans un sens ou dans l'autre qu'il n'est pas toujours facile de se forger une opinion nuancée de la question.

Depuis leur création, une des principales utilisations des réseaux P2P a été l'échange de fichiers musicaux, puis audiovisuels, entre les utilisateurs, bien souvent de manière illicite au regard des droits de propriété intellectuelle[2]. Dès lors, le « piratage » est devenu la cible privilégiée de l'industrie du disque et des sociétés de gestion collective des droits d'auteur qui n'ont pas tardé à réagir sur le terrain judiciaire contre des éditeurs de logiciels, puis contre des utilisateurs, avec plus ou moins de succès.

L'affaire qui nous occupe, intentée par la Sabam en juin 2004[3], constitua la première action du genre intentée contre un fournisseur d'accès à internet, la société Tiscali (devenue Scarlet). Sous les formes de l'action en cessation prévue à l'article 87 de la L.D.A.[4], la Sabam demandait principalement à la juridiction présidentielle de constater l'existence d'atteintes au droit d'auteur sur les œuvres appartenant à son répertoire sur le réseau de Tiscali et au moyen de logiciels P2P, et d'entendre cette dernière condamnée à les faire cesser, en paralysant l'envoi ou la réception par ses clients desdites œuvres, sous astreinte. Ce fut une première victoire, le juge acceptant de constater les atteintes au droit d'auteur et le principe d'un ordre de cessation, à condition que celui-ci soit efficace ; s'estimant trop peu informé à ce sujet, il désigna un expert chargé d'analyser la faisabilité technique d'un tel système de filtrage. Par un jugement du 29 juin 2007[5], il fit finalement droit à la demande de la Sabam.

Cette décision inédite suscite le plus grand intérêt chez les fournisseurs d'accès internet comme chez les ayants

[1] Http ://bulles.agora.eu.org/20070714_la_sabam_contre_le_P2P.html.

[2] Ce n'est évidemment pas leur seul usage, et il est important de le rappeler. Ainsi, le mouvement du logiciel « libre » s'appuie sur les réseaux P2P pour distribuer ses programmes, les éditeurs concernés n'ayant pas les ressources pour installer un serveur central (fort coûteux vu la bande passante nécessaire) les proposant en téléchargement. Ainsi, les distributions du système d'exploitation Linux s'échangent principalement par BitTorrent.

[3] Civ. Bruxelles, réf., 26 novembre 2004, *J.T.*, n° 6172, 10/2005, pp. 165 et s.

[4] Loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, *M.B.*, 27 juillet 1994.

[5] Civ. Bruxelles, cess., 29 juin 2007, R.G. n° 04/8975/A.

droit. À l'heure où ces derniers envisagent de l'utiliser comme précédent à l'échelle européenne[6], il paraît important de se pencher sur les questions, tant juridiques que techniques, qu'elle soulève.

ATTEINTE AU DROIT D'AUTEUR ET ORDRE DE CESSATION

Avant d'examiner les difficultés techniques et juridiques liées à la mise en œuvre de l'ordre de cessation, quelques réflexions s'imposent à propos de cette action en elle-même.

Tout d'abord, la Sabam justifie-t-elle d'un intérêt à agir contre Tiscali, étant entendu qu'elle ne lui reproche aucune atteinte au droit d'auteur ? Cette question a déjà été résolue, par l'affirmative, dans le jugement de 2004. D'abord, la formulation large de l'article 87 de la L.D.A. (« le juge constate et ordonne la cessation de toute atteinte au droit d'auteur ou à un droit voisin ») n'exige pas que l'action soit dirigée contre l'auteur de ces atteintes. Ensuite, de façon plus explicite, l'article 8.3 de la directive 2001/29[7] (directive « Droit d'auteur dans la société de l'information ») réserve la possibilité de requêtes « contre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou un droit voisin », et le considérant 59 de cette même directive ajoute que dans de nombreux cas, ces intermédiaires sont les mieux à même de mettre fin à ces atteintes. Le juge estime donc qu'il faut interpréter le droit belge à la lueur des textes européens, d'autant que la non-transposition de cet article en droit belge indique que le législateur considérait l'arsenal judiciaire existant suffisant. Signalons pour l'avenir que le principe est désormais consacré dans la loi sur le droit d'auteur[8].

Peut-on cependant, par un ordre de cessation (soit dans son acception usuelle une injonction de ne pas ou de ne plus faire) ordonner une mesure positive prévenant une violation future ? Ici aussi la réponse positive semble s'imposer tant en droit belge[9] qu'en droit européen : le considérant 45 de la directive 2000/31[10] (directive « Commerce électronique ») réserve la possibilité d'actions en cessation de différents types dirigées contre les intermédiaires, pouvant « notamment revêtir la forme de décisions de tribunaux ou d'autorités administratives exigeant qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible ». Nous verrons cependant par la suite que les caractéristiques de l'action en cessation telle que nous la connaissons en Belgique peuvent poser problème par rapport au régime mis en place par le législateur européen.

À supposer établie la possibilité d'une action en cessation, elle consisterait, pour le juge, à constater l'existence d'atteintes au droit d'auteur, c'est-à-dire d'établir préalablement une contrefaçon avérée, réalisée par une personne déterminée, d'une œuvre protégée par des droits dont est investi un auteur déterminé[11]. En l'espèce, l'atteinte semble supposée plus que constatée. Faisant référence à « l'abondante couverture médiatique », au « débat de société soulevé en France », le juge considère « qu'il n'existe aucune raison de croire que Tiscali serait épargnée par le phénomène », et en déduit « qu'est établie l'existence d'atteintes au droit d'auteur sur les œuvres musicales faisant partie du répertoire de la Sabam du fait de l'échange non autorisé de fichiers électroniques musicaux grâce à des logiciels *peer-to-peer* et ce, au travers de l'utilisation du réseau internet de Tiscali ». Le moins que l'on puisse dire, c'est que le constat manque de précision. Certes, dans

6 Les dispositions législatives en cause dérivent pour la plupart du droit européen ; elles sont donc largement harmonisées à travers l'Union.

7 Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, *J.O.C.E.* n° L 167 du 22 juin 2001, pp. 10-19.

8 Nouvel article 86*ter*, inséré par la loi du 9 mai 2007, *M.B.*, 10 mai 2007 : « le juge peut également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur ou à un droit voisin ».

9 Cass., 6 décembre 2001, *A&M,* 2002, p. 146 et la note de B. Michaux. Voy. aussi F. de Visscher et B. Michaux, *Précis du droit d'auteur et des droits voisins,* Bruxelles, Bruylant, 2000, n° 636.

10 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.C.E.* n° L 178 du 17 juillet 2000, p. 1.

11 E. Montero et Y. Cool, « Le *peer-to-peer* en sursis », *R.D.T.I,* n° 21, 2005, pp. 89-106.

le cas présent, il paraît superflu d'exiger une preuve plus précise tant l'existence de telles atteintes semble certaine; il n'empêche, ce glissement de la probabilité vers l'existence, sans s'en justifier spécialement, ne manquera pas d'interpeller les juristes. Surtout, l'absence de précision quant à la nature et l'étendue des infractions reprochées pourrait poser des problèmes au stade de la mise en œuvre du jugement, et entretenir l'idée que tout transfert d'œuvres du répertoire de la Sabam via un système P2P est nécessairement illicite. Au risque, une fois de plus, d'oublier purement et simplement l'existence d'exceptions aux droits exclusifs des auteurs[12].

Ayant constaté l'existence d'atteintes au droit d'auteur, le juge estime donc qu'il doit en prononcer la cessation, à condition que cet ordre mette effectivement fin à la situation illicite. Deux ans et demi et un rapport d'expert plus tard, le juge ordonne donc à Scarlet de « faire cesser les atteintes au droit d'auteur constatées dans le jugement du 26 novembre 2004 en rendant impossible toute forme, au moyen d'un logiciel P2P, d'envoi ou de réception par ses clients de fichiers électroniques reprenant une œuvre musicale du répertoire de la Sabam, sous peine d'une astreinte de 2 500 EUR par jour où Scarlet ne respecterait pas le jugement après l'expiration d'un délai de 6 mois ».

Cette formulation très large pose question. Elle opère un glissement dangereux qui tend, *de facto*, à mettre le F.A.I. dans la peau du juge. Que lui est-il demandé, sinon de constater et de faire cesser les atteintes au droit d'auteur qui ont lieu via son réseau ? Les termes de l'article 87 de la L.D.A. s'y retrouvent. Par cette injonction tout à fait générale, elle rend l'intermédiaire non seulement exécutant, mais aussi juge de milliers d'actes de cessation futurs.

FAISABILITÉ TECHNIQUE DU FILTRAGE P2P

Dans cette section, nous allons examiner la faisabilité technique d'une solution de filtrage des réseaux *peer-to-peer*. Nous n'avons pas pu examiner le rapport de l'expert désigné par le juge, dont nous ne connaissons que quelques éléments au travers du jugement. Nous avons néanmoins pris connaissance de trois documents français :

– le rapport réalisé par Capgemini en juillet 2004 pour le compte du S.N.E.P. (syndicat national de l'édition phonographique), intitulé « Étude d'outils de filtrage sur les réseaux à haut débit »[13] ;

– le rapport « Étude des solutions de filtrage des échanges de musique sur internet dans le domaine du *peer-to-peer* » d'Antoine Brugidou, directeur-associé chez Accenture et Gilles Kahn, président de l'I.N.R.I.A. (Institut national de recherche en informatique et en automatique) à la demande du gouvernement et dans le cadre de la charte « musique et internet », signé en juillet 2005 par les professionnels de la musique et de l'internet[14] ;

– le rapport rédigé en avril 2007 par Jean Cédras, avocat général à la Cour de cassation à la demande du ministre de la culture et de la Communication, à propos de la répression de la contrefaçon à grande échelle sur internet[15].

Différents types de filtrage

Le filtrage des réseaux P2P recouvre des réalités différentes. Le jugement retient onze systèmes de filtrage, dont sept seraient applicables à Scarlet. Pour simplifier, nous diviserons ces systèmes en deux niveaux et trois catégories.

Le filtrage peut intervenir à deux niveaux. Il peut d'abord être installé sur la machine de chaque utilisateur, et contrôler les communications entrantes et sortantes effectuées par ce poste. C'est la solution la plus économique, et sans doute la plus efficace, mais elle est confrontée à un obstacle de taille : on ne peut pas contraindre les utilisateurs particuliers à installer un tel système. Utilisé sur une base volontaire, il ne permet donc pas de répondre au piratage à grande échelle.

Le second niveau est celui du fournisseur d'accès à internet (F.A.I.), qui est l'intermédiaire entre l'internaute et le Web (c'est le cas de Scarlet). Ici, le problème

12 I. Schmitz, « Le *peer-to-peer* ou le réveil de Robin des Bois », première publication sur http://www.droit-technologie.org, p. 8 : « Le téléchargement peut dans certaines conditions constituer une copie privée ».

13 http://www.lesechos.fr/lettrespro/presentation/telecom/flash/rapport_filtrage_capgemini_france.pdf.

14 http://160.92.130.199/discours/2005/musiqueinternet.htm.

15 http://www.odebi.org/docs/RapportCedras.pdf.

principal est le volume du trafic. Le F.A.I. doit relayer les informations émises et reçues par tous ses clients, ce qui représente un volume de données considérable à chaque instant. Une solution de filtrage doit être capable d'analyser toutes ces données sans pour autant ralentir le trafic, ce qui nécessite de toute façon des machines très performantes, et donc des investissements conséquents.

Mais il faut encore savoir ce que l'on va filtrer, et surtout quel critère va utiliser le filtre pour discriminer les données. Trois catégories sont ici envisageables : le filtrage par port, le filtrage par protocole et le filtrage par contenu.

Le filtrage par port est la solution la plus basique. Un port peut être vu comme une porte d'entrée vers l'ordinateur. L'ouverture de plusieurs de ces portes permet à l'ordinateur d'effectuer différents types de communications simultanément. Le filtrage consiste donc à fermer les portes qui sont utilisées par les logiciels P2P pour communiquer entre eux. Cette solution est cependant écartée par tous les rapports : les programmes P2P modernes sont capables d'utiliser différents ports, dont ceux utilisés pour le trafic internet « normal », et qui sont donc impossibles à fermer sous peine de couper tout accès à internet.

Le filtrage par protocole consiste à analyser les paquets de données échangés entre les ordinateurs. Ceux-ci contiennent une « signature » permettant au logiciel P2P de reconnaître ces données comme lui étant destinées, pour les interpréter ensuite. Le filtrage détecte ces signatures et peut ensuite bloquer l'échange des données. Cette solution n'est pas satisfaisante pour deux raisons.

D'abord elle ne répond pas à la problématique spécifique du piratage d'œuvres protégées : ce type de filtrage est uniquement capable de détecter, puis de bloquer, des échanges de données effectués au moyen d'un logiciel P2P, sans prendre connaissance du contenu de ces échanges. Il n'est donc pas question de bloquer les fichiers illicites, mais bien la totalité du trafic P2P.

Ensuite, elle montre déjà ses limites d'un point de vue technique. D'abord par les investissements qu'elle demande, et ensuite parce que les logiciels P2P sont déjà capables de le contourner. Ainsi, après l'installation d'un tel filtrage par le F.A.I. français Free[16], il n'a fallu que très peu de temps pour qu'apparaisse sur les clients vedettes eMule et BitTorrent une option de « brouillage du protocole », qui permet de masquer la signature des paquets et de contourner le filtre[17]. Certes, des équipementiers affirment aujourd'hui pouvoir neutraliser ce brouillage, notamment en analysant le comportement des paquets de données, mais de telles solutions n'ont pas été testées à grande échelle, et risquent, elles aussi, d'être contournées tôt ou tard. Pour ces deux raisons, le filtrage systématique du protocole a été jugé « difficile » dans le rapport Brugidou & Kahn.

Le filtrage par contenu est considéré par l'expert judiciaire comme « le seul à tenter de répondre à la problématique de façon spécifique ». À l'heure actuelle, il n'existe qu'un système permettant ce type de filtrage : le « CopySense Network Appliance » développé par la société Audible Magic[18]. C'est de fait la seule solution envisagée dans le jugement, et donc celle qui devrait être mise en œuvre par Scarlet.

Filtrage par contenu, une solution satisfaisante ?

Le système Audible Magic a été développé pour les universités, écoles et entreprises qui souhaitent que leurs réseaux ne soient plus utilisés comme plaques tournantes de téléchargements illicites. Il repose sur l'utilisation de *fingerprints* des morceaux de musiques. Il effectue d'abord une copie de tout le trafic traversant le réseau, puis, en analysant des courts extraits des morceaux transmis, il détermine leur « empreinte », unique, qu'il compare ensuite à une base de données gigantesque reprenant les « empreintes » des morceaux protégés par le droit d'auteur. S'il reconnaît le morceau transmis, il bombarde l'émetteur et le destinataire de faux paquets de données, provoquant des erreurs et interrompant la connexion.

16 Il n'était pas question ici de lutte contre le piratage, mais de limiter l'utilisation de bande passante utilisée par le P2P, jugée excessive par Free, afin de ne pas ralentir le reste du trafic internet.

17 Pour plus d'infos, voy. http://www.emule-project.net/home/perl/help.cgi?l=13&rm=show_topic&topic_id=851.

18 http://www.audiblemagic.com.

Les obstacles techniques à la mise en œuvre sont ici encore plus importants[19]. Premièrement, le programme doit distinguer le trafic P2P du trafic «normal», et analyser le seul premier. Cela nécessite en soi un filtrage du protocole, avec les difficultés dégagées ci-dessus. Ensuite, les boîtiers CopySense ne peuvent traiter qu'un trafic limité, de l'ordre de 300 Mb/s., ce qui implique pour le F.A.I. l'obligation de diviser le trafic entre les différents boîtiers. Ainsi, le modèle réalisé par Brugidou & Kahn prévoit l'utilisation moyenne d'un boîtier pour 10 000 abonnés, en prévoyant que la tendance à l'augmentation de la bande passante et la généralisation des services de transfert de voix et de vidéo vont sans doute augmenter significativement la bande passante générée par chaque utilisateur (plusieurs centaines de Kbps, contre une trentaine maintenant). Ainsi, outre leur propre coût, les boîtiers Audible Magic nécessitent des équipements de découpage du trafic, et nuiraient potentiellement à l'installation au niveau des F.A.I. d'appareils permettant un élargissement de la bande passante, et donc l'augmentation de la vitesse des transmissions pour les internautes.

Les avis des experts convergent sur la faisabilité d'une mise en œuvre d'un filtrage par contenu au niveau du F.A.I.: le rapport CapGemini le juge irréalisable, le rapport Brugidou & Kahn, «non pertinent» dans le cadre d'un filtrage systématique et même «peu pertinent» dans le cadre d'un filtrage à la demande qui ne concernerait que 10% des utilisateurs, et enfin l'expert judiciaire ne le considère «pas dimensionné pour répondre au volume de trafic d'un F.A.I., ce qui induirait un coût d'acquisition et d'exploitation élevé pour compenser ce sous-dimensionnement».

Dès lors, on ne peut que s'étonner de voir le juge considérer cette solution applicable à Scarlet, d'autant que, rappelons-le, il n'existe pas actuellement d'autre possibilité de filtrage par contenu. Certes, comme le remarque le juge, Audible Magic est utilisé par des géants de l'internet comme MySpace ou YouTube mais l'utilisation en est complètement différente. Ces sites permettent aux utilisateurs de stocker leurs fichiers audio ou vidéo, qui seront ensuite hébergés et rendus accessibles aux autres internautes. Il ne faut donc analyser un fichier qu'une fois, lorsqu'un utilisateur l'envoie pour le stocker. Cela nécessite, on s'en doute, beaucoup moins de ressources que d'analyser tout le trafic internet entrant et sortant chez tous les clients d'un F.A.I. Pour le surplus, l'efficacité de ce système semble encore incertaine[20].

Toute aussi étonnante est la position du juge à propos du chiffrement des données, rendant celles-ci illisibles par toute autre personne que le destinataire. Il est soulevé par tous les experts comme une menace réelle pour la pérennité d'un système de filtrage de contenu, et pourtant balayé par le juge: «la question d'un cryptage futur éventuel ne peut aujourd'hui faire obstacle à une mesure de cessation […] le juge des cessations ne peut tenir compte de spéculations sur des évolutions techniques futures éventuelles». C'est d'autant plus étonnant que les possibilités de chiffrement ne sont ni futures, ni éventuelles. Des logiciels P2P permettant une utilisation anonyme et sécurisée existent depuis plusieurs années[21] [22]. Ils utilisent les mêmes technologies de cryptographie que celles utilisées en commerce électronique pour sécuriser les transactions. Si leur diffusion reste confidentielle, c'est probablement parce que la nécessité de les utiliser ne s'est pas encore fait sentir pour le large public des non-connaisseurs.

Enfin, le coût devant être supporté par Scarlet pour installer un système de filtrage ne semble pas excessif au juge. L'expert judiciaire l'évalue à 0,5 EUR/abonné/mois pour une période de 3 ans; le rapport Brugidou & Kahn parle de 4,4 EUR/abonné pour l'achat des seuls boîtiers, les coûts supplémentaires pouvant être significatifs et beaucoup plus importants au final que le coût des boîtiers[23]. Le coût du filtrage tournerait donc autour du million d'euro par an, sans compter l'augmentation de trafic qui se produit chaque année, pour Scarlet (qui ne représente qu'un modeste 4% du marché belge). Le filtrage de tout le trafic belge coûterait aux fournisseurs d'accès, donc aux internautes, environ 25 millions d'euros par an sans rapporter, à ce stade, la moindre contribution financière aux titulaires de droits.

[19] Pour un modèle de mise en œuvre d'Audible Magic chez un F.A.I., voy. rapport Brugidou & Kahn, p. 51.

[20] http://newteevee.com/2007/06/08/does-digital-fingerprinting-work-an-investigative-report/.

[21] Citons pour exemples les projets Share, Mute, Ants et Freenet.

[22] http://www.eff.org/share/audible_magic.php?f=audible_magic2.html.

[23] Rapport Brugidou & Kahn, *op. cit.*, p. 54.

D'un point de vue strictement technique, la solution Audible Magic paraît donc coûteuse, difficile à mettre en place, et peu fiable. Nous doutons que sa mise en œuvre soit à même de satisfaire le dispositif du jugement, formulé de manière large.

OBSTACLES JURIDIQUES

Questions posées par la directive 2000/31

Nous avons déjà évoqué plus haut les dispositions de droit européen qui prévoient la possibilité d'une action contre un F.A.I. afin de faire cesser ou de prévenir un trouble dont il n'est pas l'auteur. Il convient à présent de les replacer dans un cadre plus large, celui du régime de la responsabilité des intermédiaires sur internet.

La directive « commerce électronique » tente en effet de concilier au mieux les intérêts des différentes parties, dans un fragile équilibre visant à ne pas imposer de charge déraisonnable aux intermédiaires, tout en permettant l'exploitation des moyens dont ils disposent[24]. Ainsi interdiction est faite aux États membres d'imposer aux intermédiaires une obligation générale de surveiller le réseau (article 15), et leur responsabilité pour les informations qu'ils transmettent ou stockent temporairement est exonérée (articles 12 et 13). D'autre part, les États membres peuvent requérir leur collaboration pour informer les autorités d'activités illicites dont ils auraient connaissance (article 15.2), et pour mettre un terme à une violation suite à une injonction (articles 12.3 et 13.2, déjà évoqués). Les considérants 40 à 48 de la directive détaillent cet équilibre de façon éloquente. Il nous semble que le jugement du 29 juin 2007 est de nature à le compromettre significativement.

Obligation générale de surveillance

Reprenant la directive, la loi belge de 2003[25] indique que « les prestataires n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites », tout en n'empêchant pas « les autorités judiciaires compétentes d'imposer une obligation temporaire de surveillance dans un cas spécifique, lorsque cette possibilité est prévue par une loi »[26].

Le juge considère cependant que « l'ordre de cessation n'impose pas à Scarlet de " surveiller " son réseau, et que les solutions identifiées par l'expert sont des " instruments techniques " qui se limitent à bloquer ou à filtrer certaines informations qui sont transmises sur le réseau de Scarlet ; qu'elles ne sont pas constitutives d'une obligation générale de surveiller le réseau ». Voilà qui laisse perplexe quant on sait que le jugement oblige Scarlet à « faire cesser les atteintes au droit d'auteur en rendant impossible toute forme d'envoi ou de réception [des œuvres de la Sabam] ». En effet, pour bloquer ces échanges de données, il faut nécessairement les détecter. Et pour les détecter, il faut nécessairement analyser tous les échanges.

Pour le surplus, rappelons en quelques mots le fonctionnement du système Audible Magic : après avoir isolé le trafic P2P du reste, il fait une copie de toutes les données transmises qu'il compare ensuite à une base de données reprenant les œuvres protégées. Il interrompt enfin l'échange s'il a reconnu une œuvre.

Certes, le considérant 40 de la directive indique que cette disposition ne doit pas faire obstacle à la mise en œuvre « d'instruments techniques de surveillance », mais nous pensons qu'il ne faut y voir qu'une confirmation de la possibilité, pour les F.A.I., d'installer des équipements de surveillance nécessaires à la sécurité et au bon fonctionnement de leur réseau. À suivre le juge, l'imposition d'une surveillance effectuée par un « instrument technique » serait autorisée. Cela revient purement et simplement à vider l'article 15 de sa substance puisqu'il ne pouvait qu'être évident pour les rédacteurs de la directive qu'une « obligation générale de surveillance » ne peut se faire qu'au moyen d'équipements techniques dans l'environnement numérique.

La loi du 11 mars 2003 précise qu'une obligation de surveillance ne peut être que spécifique et temporaire. L'ordre de cessation, tout à fait général et dépourvu de limitation dans le temps, semble donc beaucoup trop large au vu des conditions légales.

---

[24] E. Montero, « La responsabilité des prestataires intermédiaires sur les réseaux – Le commerce électronique sur les rails », *Cahiers du C.R.I.D.*, n° 19, Bruxelles, Bruylant, 2001, p. 279.

[25] Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003.

[26] Article 21.

Exonération de responsabilité

L'article 12.1 de la directive dispose que « les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire :

a) ne soit pas à l'origine de la transmission ;
b) ne sélectionne pas le destinataire de la transmission, et
c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission ».

Le juge s'appuie toutefois sur l'article 12.3, qui précise « le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative […] d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation ». Il ajoute de surcroît que « ces dispositions qui règlent ainsi la responsabilité du prestataire s'adressent exclusivement au juge de la responsabilité et sont sans incidence sur le présent litige dans la mesure où l'action en cessation ne suppose aucun constat préalable d'une faute dans le chef de l'intermédiaire ».

Le droit européen réserve donc les actions « en cessation »[27] à l'encontre d'un intermédiaire. L'emploi de ce terme peut porter le juriste belge à confusion, car il semble que le législateur européen n'ait entendu viser que les actions au provisoire permettant d'ordonner le retrait d'informations illicites[28]. Or, les actions en cessation telles que nous les entendons en droit belge ont une portée qui dépasse le provisoire. Le juge s'y prononce sur le fond, de manière définitive et dans une mesure qui lie le juge appelé à se prononcer sur la responsabilité. Dès lors, il serait logique que l'exonération de responsabilité s'applique également aux procédures en cessation[29], du moins lorsqu'elles amènent à établir une violation de la loi, constitutive de faute, dans le chef d'un intermédiaire de l'Internet.

De plus, la directive n'accorde l'exonération de responsabilité qu'à certaines conditions rappelées ci-dessus, et en particulier que l'intermédiaire ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission. Est-ce toujours le cas dans un scénario où Scarlet analyse toutes les informations qu'il transmet, et en sélectionne certaines (les œuvres protégées), qu'il bloque ? Il nous semble que non[30] : à partir du moment où il sélectionne les informations qu'il transmet, il prend un rôle actif et pourrait perdre le bénéfice de l'exonération de responsabilité. Celle-ci serait alors engagée s'il transmet des informations illicites, ou s'il bloque des informations licites. Non, affirme le juge, car « la mesure de blocage [est] purement technique et automatique, l'intermédiaire n'opérant aucun rôle actif dans le filtrage ». Devons-nous en déduire que si la sélection est opérée par un dispositif technique, ce n'est pas l'intermédiaire qui l'effectue ? Conclusion plus que discutable, encore une fois.

La directive 2000/31 a construit un système dans lequel « les intermédiaires techniques n'ont qu'à se soucier de collaborer avec la justice, sans devoir traquer eux-mêmes les infractions »[31]. En donnant aux fournisseurs d'accès un rôle beaucoup plus actif, la décision présidentielle s'écarte largement de cette conception, au risque de la faire voler en éclats.

Questions posées par les directives 1995/46[32] et 2002/58[33]

Traitement de données à caractère personnel

Le juge commence par affirmer que les logiciels de filtrage et de blocage ne traitent en tant que tels

27 Terme utilisé dans le considérant 45 de la directive.

28 A. Cruquenaire et J. Herveg, « La responsabilité des intermédiaires de l'Internet et les procédures en référé ou comme en référé, note sous Liège, 1re ch., 28 novembre 2001 », *J.T.*, 2002, pp. 308-311.

29 A. Cruquenaire et J. Herveg, *op. cit.*, p. 310 ; dans le même sens, voy. A. Strowel, N. Ide et F. Verhoestraete, « La directive du 8 juin 2000 sur le commerce électronique : un cadre juridique pour Internet », *J.T.*, 2001, pp. 141 et 142, n° 32.

30 Dans le même sens, E. Montero et Y. Cool, *op. cit.*, p. 103.

31 E. Montero et Y. Cool, *op. cit.*, p. 103.

32 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.* n° L 281 du 23 novembre 1995, pp. 31-50.

33 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection

aucune donnée à caractère personnel. Nous contestons cette analyse. Le système Audible Magic prend connaissance des adresses IP de l'émetteur et du récepteur de la communication, enregistre ces données ainsi que les événements qu'il génère (blocage d'une communication, par exemple). Il mentionne d'ailleurs *monitoring users* et *log and report* comme une de ses trois fonctions principales.

La loi du 8 décembre 1992[34], reprenant la directive, qualifie de donnée à caractère personnel toute information concernant une personne identifiée ou identifiable, c'est-à-dire qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification, par quelque moyen qui puisse être raisonnablement mis en œuvre. L'adresse IP, attribuée par le fournisseur d'accès à son abonné pour la durée de la connexion, tombe donc certainement sous cette définition, puisque le F.A.I. est en mesure de faire le lien entre l'adresse IP et la personne. Cet avis est partagé tant par la Commission de protection de la vie privée[35] que, plus récemment, par le président du groupe « article 29 »[36] devant le parlement européen et par l'avocat général Kokott dans ses conclusions[37] dans l'affaire *Promusicae*[38], qui n'ont pas été démenties par la Cour.

Le juge prend d'ailleurs soin au paragraphe suivant de donner une justification à ce (non-)traitement de données à caractère personnel : l'article 5, b), de la loi de 1992 autorise le traitement de données nécessaire à l'exécution d'un contrat auquel la personne concernée est partie. Les conditions générales de Scarlet interdisant notamment à ses abonnés d'utiliser son réseau en violation des droits d'auteur, sous peine de sanctions, le filtrage serait « nécessaire à l'exécution du contrat ». On peut douter de cette justification qui paraît un peu légère. La « nécessité » est-elle établie alors que l'absence de mesures de filtrage n'a nullement empêché l'exécution des contrats de fourniture d'accès à internet durant plusieurs années ? Le contrat entre le F.A.I. et ses clients peut-il être invoqué par un tiers pour imposer un traitement dont le premier ne veut pas ?

Mais, plus fondamentalement, le raisonnement du juge nous semble critiquable. En effet, l'article 5 de la loi de 1992 énonce limitativement les cas dans lesquels un traitement de données peut être effectué. Par qui ? Par le responsable de traitement ou pour son compte[39] ; celui-ci est défini à l'article 1er, § 4, comme « la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ». Il ne s'agit donc pas nécessairement de celui qui effectue le traitement dans les faits. Dans l'affaire qui nous occupe, il nous paraît tout à fait raisonnable de considérer que c'est la Sabam qui en détermine les finalités et les moyens.

Dès lors, c'est dans son chef qu'une des conditions de l'article 5 doit être remplie pour que le traitement soit autorisé, la seule envisageable étant celle prévue à l'alinéa f) : « lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi ». Ceci implique, à tout le moins, une balance d'intérêts qui aurait dû être effectuée par le juge.

Enfin, même si le traitement est autorisé par la loi de 1992, il se doit de respecter les conditions strictes qu'elle pose et notamment le principe de proportionnalité qui stipule expressément que les données collectées doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement »[40]. À cet égard, il est permis de douter

de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.* n° L 201 du 31 juillet 2002, pp. 37-47.

34 Loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel.

35 Avis n° 44/2001, avis d'initiative concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications.

36 http ://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm.

37 Conclusions de l'avocat général Mme Juliane Kokott présentées le 18 juillet 2007.

38 C.J.C.E., 29 janvier 2008, aff C-275/06 *Promusicae*.

39 On en trouve une illustration à l'article 4, § 2.

40 Loi du 8 décembre 1992, article 4, § 1er, 3°.

de la proportionnalité par rapport aux finalités d'une surveillance systématique de toutes les communications des internautes[41].

Secret des communications

L'article 5 de la directive 2002/58 (directive « Vie privée et communications électroniques ») garantit la confidentialité des communications[42]. Les États membres sont tenus, en particulier, « d'interdire à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, § 1er ».

Le système Audible Magic, on l'a vu, vise à prendre connaissance du contenu des communications P2P pour identifier, le cas échéant, des morceaux de musique déterminés. Il s'agit donc très certainement d'un système de surveillance, d'interception ou d'écoute au sens de cet article. Système qui ne serait autorisé par l'article 15, § 1er, « qu'en vertu d'une mesure législative qui constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ». Cet article se réfère en outre explicitement à l'article 13, § 1er, de la directive 95/46. Il faut donc en déduire que les États membres peuvent prendre des mesures limitant l'obligation de confidentialité des données personnelles lorsque cette limitation est nécessaire pour la protection des droits et libertés d'autrui, notamment le droit d'auteur, protégé au titre du droit de propriété[43]. Mais encore une fois, il importait que les droits fondamentaux à la protection de la vie privée et à la protection de la propriété soient mis en balance par le juge.

La technologie ne connaît pas le droit

Plus fondamentalement, et au-delà des questions précises soulevées ci-dessus, la licéité d'une communication est une donnée étrangère à la technique. Or, il est demandé à Scarlet de faire cesser les atteintes au droit d'auteur, soit de bloquer les échanges illicites. C'est là que le bât blesse : un système de filtrage, aussi perfectionné soit-il, n'est pas capable à l'heure actuelle d'identifier une œuvre, ses ayants droit, l'émetteur et le destinataire de la communication, et de déterminer si ces deux derniers ont obtenu l'autorisation du premier, ou encore s'ils peuvent se prévaloir d'une exception au droit d'auteur rendant leur échange licite.

Certes, le champ des exceptions n'est pas très large, et il tend à se réduire encore, malmené par la directive 2001/29 (directive « Droit d'auteur et société de l'information ») et son redoutable « test des trois étapes »[44]. Il n'empêche, le dispositif du jugement (ordonnant de rendre impossible toute forme d'envoi ou de réception [des œuvres de la Sabam]) revient à nier purement et simplement la possibilité d'un échange licite d'une œuvre appartenant au répertoire de la Sabam via le réseau internet. Le juge prend d'ailleurs acte de ce risque de blocage de transmissions licites, sans guère s'émouvoir de ces dommages collatéraux.

La technologie doit être utilisée pour ce qu'elle est et pour ce qu'elle sait faire. Dans son état actuel, elle ne sait pas appliquer le droit. Lui demander de le faire conduit nécessairement à des imperfections, plus ou moins dérangeantes. À oublier cette notion fondamentale, les « victimes collatérales » de ce genre de procès risquent de se multiplier.

CONCLUSION

La difficulté du droit des technologies de l'information et des communications, on le sait, tient souvent à la bonne compréhension des phénomènes techniques concernés

41 Dans ce sens, T. Verbiest et M. de Bellefroid, « Filtrage et responsabilité des prestataires techniques de l'internet : retour sur l'affaire *Sabam c. Tiscali* », *Légipresse*, n° 246, novembre 2007, pp. 156 à 160.

42 Une « communication » étant définie comme toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Un échange de fichier par un système P2P est certainement une « communication ».

43 C.J.C.E., 29 janvier 2008, aff. C-275/06 *Promusicae*, point 53.

44 Sur cette notion, voy. I. Schmitz, « Le *peer-to-peer* ou le réveil de Robin des Bois », *J.T.*, 7/2001, p. 165.

et de leurs implications afin de leur appliquer correctement les règles juridiques. Il nous semble que, dans ce jugement, la réalité technique n'a pas été suffisamment prise en compte. Le filtrage des réseaux P2P n'agit pas comme un filtre à café, qui séparerait mécaniquement les transmissions illicites, du trafic autorisé. Il implique la mise en place de mécanismes complexes, pouvant utiliser différents critères dont aucun n'est totalement pertinent pour juger de la licéité de la communication, et qui entraînent la surveillance de tous les utilisateurs du réseau et du contenu des informations qu'ils s'échangent, et la censure de certaines de leurs communications.

Simple « filtre » dans l'esprit du juge, les dispositifs envisagés ont des implications qui ne peuvent être passées sous silence, en termes de respect des droits fondamentaux comme la vie privée ou de liberté d'expression. Ils menacent également les équilibres fragiles instaurés par le législateur européen à propos de la répartition des responsabilités sur internet.

Bien sûr, notre propos ici n'est pas de nier les droits exclusifs que la loi reconnaît aux auteurs sur leurs créations. Mais le droit d'auteur a toujours été un droit d'équilibre, entre leurs droits et ceux des utilisateurs, entre la protection de la création et l'intérêt public. La propagation des T.I.C. bouleverse les rapports de force antérieurs, et des interventions législatives et judiciaires sont bien sûr souhaitables. Nous pensons qu'elles doivent être proportionnées et équilibrées, à l'heure où la légitimité du droit d'auteur paraît menacée. Le présent jugement soulève des écueils importants, et nous espérons que le juge d'appel y apportera des réponses satisfaisantes.